AN ANALYSIS OF FACTORS THAT HAVE INFLUENCED THE EVOLUTION OF INFORMATION ASSURANCE FROM WORLD WAR I THROUGH VIETNAM TO THE PRESENT

THESIS

Kelvin B. Scott, Gunnery Sergeant, USMC

AFIT/GIR/ENV/04M-22

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the United States Marine Corps, United States Air Force, Department of Defense, or the United States Government.

AFIT/GIR/ENV/04M-22

AN ANALYSIS OF FACTORS THAT HAVE INFLUENCED THE EVOLUTION OF INFORMATION ASSURANCE FROM WORLD WAR I THROUGH VIETNAM TO THE PRESENT

THESIS

Presented to the Faculty

Department of Systems and Engineering Management

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Information Resource Management

Kelvin B. Scott, BS, MS

Gunnery Sergeant, USMC

March 2004

AFIT/GIR/ENV/04M-22

AN ANALYSIS OF FACTORS THAT HAVE INFLUENCED THE EVOLUTION OF INFORMATION ASSURANCE FROM WORLD WAR I THROUGH VIETNAM TO THE PRESENT

Kelvin B. Scott, BS, MS
Gunnery Sergeant, USMC

Approved:

_____//SIGNED//_____	17 March 2004
Dr. Alan R. Heminger, (Chairman)	date
_____//SIGNED//_____	17 March 2004
Dr. Kevin L. Elder, (Member)	date
_____//SIGNED//_____	17 March 2004
Capt David D. Bouvin, PhD, (Member)	date

Abstract

This study is an exploratory historical analysis of the factors that have influenced the evolution of military Information Assurance (IA) programs from World War I to the present. Although the term IA has recently been widely used throughout the Information Resource Management field (IRM), evidence indicates that information and information systems protection mechanisms were used during every U.S. Military conflict. This research proposes to increase the body of knowledge within the information systems management field by exploring the areas related to Information Assurance (IA) and the ultimate goal of U. S. Defensive Information Warfare.

I found that significant events related to the protection of information and information systems security throughout each U.S. Military conflict led to the implementation of IA concepts. The evaluation of these events provides information that reveals a common approach to IA throughout history and supports the identification of key concepts that have influenced this evolutionary process and shaped the role of IA in current military operations, with indicators of how it may be used in the future.

Acknowledgements

This thesis effort could not have been completed without the help of several people who provided support and assistance throughout. First and most importantly, I would like to thank my wife and children for their unconditional love, understanding and support during the past 18 months. Their encouragement and sacrifice has made this experience less stressful and more rewarding.

Special thanks to the AFIT Marines who braved this entire program with me. We are the pioneers of the "Enlisted at AFIT" program. Your support, unselfishness, and guidance helped me through the tough times and I will be forever grateful. Semper Fidelis! I would also like to thank my thesis committee. To Dr. Heminger, for his advice and direction and giving me the academic freedom to develop my own research techniques. To Captain Bouvin for his Information Assurance "eye" by ensuring that certain concepts were pertinent and valid. To Dr. Elder for his critical thinking approaches and overall willingness to ask the difficult questions.

Finally, I would like to God. For without him, nothing is possible. You have given me the discipline and knowledge to make it through this program by overcoming my weaknesses and capitalizing on my strengths. I am forever grateful to you.

Table of Contents

Page

List of Figures

List of Tables

AN ANALYSIS OF FACTORS THAT HAVE INFLUENCED THE EVOLUTION OF INFORMATION ASSURANCE FROM WORLD WAR I THROUGH VIETNAM TO THE PRESENT

I. Introduction

Overview

World War I (WWI) introduced numerous technological advancements that revolutionized the nature of twentieth century warfare (AMH, 1989). Such advancements also paved the way for many of the Revolutions in Military Affairs (RMA) that have taken place since then. In his book, Lifting the Fog of War, Admiral Bill Owens states that "the technological base of the current RMA remains the central component of a transformed twenty-first century American fighting force." He also states that "this RMA will be the best hope for the United States to keep its armed forces superior to any other nation's (Owens, 2000)." The technological strides made from WWI forward set the stage for further advancements of military capabilities and expertise throughout the history of U.S. military operations. According to Andrew Krepinevich, RMA is described as a dynamic process:

> "An RMA occurs when the application of new technologies into a significant number of systems combines with innovative operational concepts and organizational adaptation in a way that fundamentally alters the character and conduct of conflict. It does so by producing a dramatic increase-often an order of magnitude or greater-in the combat potential and military effectiveness of armed forces" (Krepinevich, 1994: 30).

Such innovative approaches have continued to change the way military operations are conducted. This trend will likely continue well into the future.

A wide array of computer and network hardware and software that can be adaptable for military use will empower the U.S. Military to maintain combat superiority over adversaries well into the twenty-first century (Owens, 2000). This goal cannot be achieved without the highest levels of Information Assurance (IA), which provides the basic building blocks for the protection and defense of information and information systems. Joint Publication 3-13, a document developed by the Department of Defense (DOD), defines IA as the protection and defense of systems by ensuring their availability, integrity, identification, confidentiality, and non-repudiation (JP 3-13, 1998). These fundamental terms form the building blocks for successful IA. There are several different definitions of these five terms, however, Maconachy (2001), McKnight (2002), and Cummings (2002) assembled definitions that reveal key aspects of IA as characterized by this research effort.

- *Authentication* is verification of the originator. A security service designed to establish the validity of a transmission, message, or originator. It ensures that the information originated from a specific known source. It verifies the identity of the user, device, or other entity in a computer system, often as a prerequisite to allowing access to resources in a system. It ensures that you have the right to see the information, and that you are who you say you are.

- *Availability* is the assured access to data by authorized users. It is the state where information is in the place needed by the user, at the time the user needs it, and in the form needed by the user. One key is timely delivery of information and that the information presented in a form that is wanted and can be understood. Can be related to security services including back-up power, spare data channels, off site capabilities, and continuous signals.

- *Confidentiality* is the protection from unauthorized disclosure. It is the concept of holding sensitive data in confidence, limiting it to an appropriate set of individuals or organizations. Referred to as information security and addresses the issues of clearances and a need to know.

- *Integrity* is the protection from unauthorized change. It involves information or communications that are sound, unimpaired, and in perfect condition. Looks at the overall architecture of the system including how it is designed, implemented, and maintained.

- *Non Repudiation* is the undeniable proof of participation in a communication. It is a service that provides proof of the integrity and origin of data in an unforgettable relationship, which can be verified by any third party at any time. It involves a communication that is genuine and cannot be refuted. Key aspects are proof of origin, submission, and delivery.

The terms identified above can be further characterized as security concepts relating to the point to point communications or internet transmissions; confidentiality, integrity, and availability and security concepts relating to people; authentication, authorization, and non-repudiation. These terms also represent a desired end state accomplished by the overall organizational goal.

This thesis will explore the areas related to IA and the ultimate goal of Defensive Information Warfare throughout the history of the U. S. Military from WWI through Vietnam to the present. This research will be qualitative and rely on historical perspectives of various documentation and personal accounts relating to IA and building theory on the evolution of IA and the ultimate goal of information superiority (IS).

Joint Vision 2020, developed by the Joint Chiefs of Staff, defines IS as, "the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same (JV2020, 2000)." JV2020 also states that Information Superiority is a key enabler of the transformation of military

operational capability during peace and conflict (JV2020, 2000). It has been widely accepted that the one who controls the flow of information to the battlefield will emerge the victor. According to a recent research effort, this phenomenon will continue to expand the capabilities of the warfighter:

> "The proliferation of information technologies will continue to shape the behavior of military operations…unlike early military research and development where technologies were created and advanced internally, information and computing technology is largely commercialized and therefore available to all" (Knode, 2003).

The most recent capabilities of IS were seen first hand during Operation Iraqi Freedom and ongoing operations in the gulf region. Most people observed this phenomenon take shape by tuning into CNN, Fox News, or MSNBC, where they watched embedded journalists with military units, and daily updates from various military leaders. Only recently have such advances in technology been so readily available. In the past, various data was just as important, however, it took much longer to transform such data into usable information. We are now seeing first hand how information technologies have transformed military operations. The protection of these various advancements in information technologies, which assists in the formulation of communications strategies, is equally important.

The U. S. Military is an agile force capable of sustaining the technological and operational capability needed to win America's battles. The success of this technological capability will depend on IA initiatives and will ultimately lead to IS over adversaries. Normal military operations have demonstrated the constant need for IA. This need is infinitely greater once crisis or conflict become apparent. IA forms the foundation of defensive information warfare, which protects information resources from attack

(Denning, 1999: 12). The foundation of effective information operations (IO) is also imbedded in IA strategies. IA focuses on the defensive or protective aspect of information systems during Information Operations (IO). Joint Publication (JP 3-13, 1998) defines IO as actions taken to affect adversary information and information systems while defending one's own information and information systems from attack Figure 1 shows that IA is the only element of information operations represented across the entire spectrum from peace, to crises, to conflict, and back to peace again.

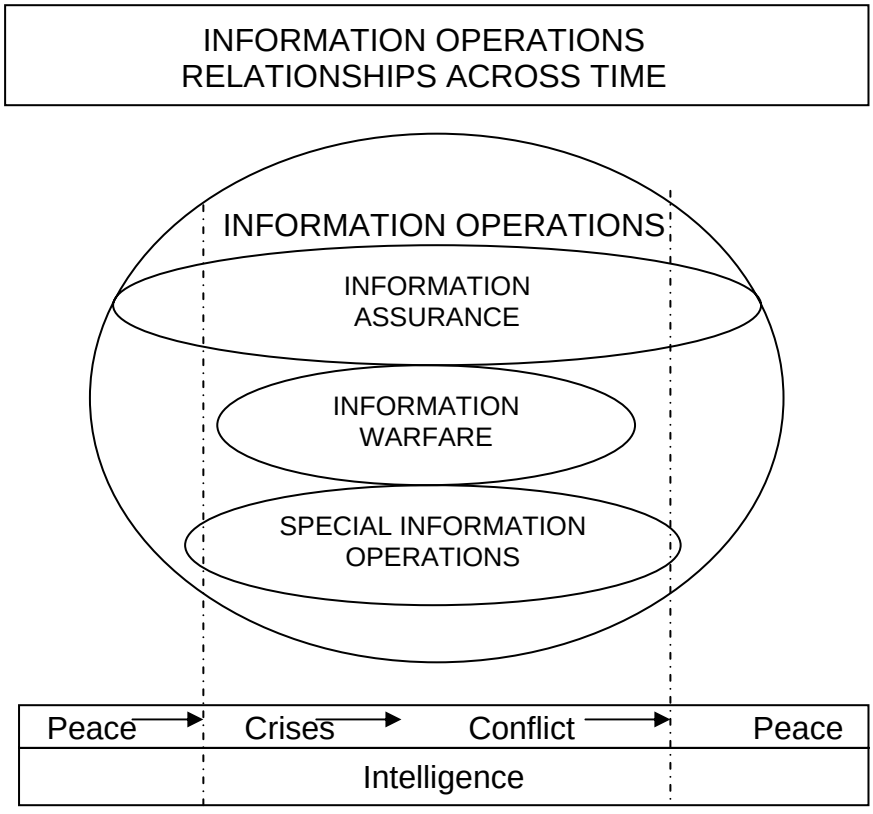

Figure 1: Relationships across time (JP 3-13, 1998: I-4)

To achieve total protection of information and information systems from attack, IA programs must meet the commander's needs across the entire spectrum of events. Additionally, IA must coexist with information warfare and special information

operations during the crises and conflict spectrum. This relationship must be dynamic and complementary to ensure the highest degree of dominance. Although this strategy has only recently been identified as such, military operations in the past have also relied on a similar operational activities that ensure appropriate levels of IO

Some aspects of IO will only take place during crises and conflict and others will take place at various stages throughout the entire spectrum. IA must occur throughout because the basic defensive measures will often help prevent crisis and conflict. Although this format is only recently been incorporated into military doctrine, current military leaders indicate that IO in relation to IA has always been structured similarly (JP 3-13, 1998: II-8).

Problem Statement

Although the term IA has only recently been widely used throughout the Information Resource Management field (IRM), there is a strong indication that information and information system protection mechanisms were used during every U.S. Military conflict from WWI forward and that the ultimate goal of IS has lead to a certain level of IA throughout. To understand its importance, it may be valuable to trace IA related concepts back through various military conflicts. The evaluation of these conflicts can be used to provide key characteristics of IA throughout that time. This research effort will explore how past military conflicts have also relied on IA during defensive information warfare as far back as WWI even though such efforts were not referred to as IA. The goal will be the identification of concepts that have influenced this

evolutionary process and shaped the role of IA in current and future military environments.

Research Question

IA is expected to be an integral element in the process that leads to IS in future military operations. Since this goal of achieving IS will continue to be paramount, it may be useful to explore the role of concepts related to the protection of information and information systems in past and current military operations and how such concepts will influence the future. What are the factors that have influenced the evolution of IA from WWI through Vietnam to the present?

Investigative Questions

1. Prior to the establishment of IA programs, what key programs were established to protect information and information systems in the U.S. Military from WWI through Vietnam to the present?
2. What is an appropriate evolutionary model of IA given military operations from WWI through Vietnam to the present?
3. What lessons can we learn from the implementation of IA programs and the evolutionary model of IA?

Methodology

The research methodology chosen for this thesis effort will center on historical research techniques. According to Nel (1983), historical research is:

> "The systematic process of collecting and objectively evaluating data related to past occurrences to arrive at conclusions about the causes, effects, or trends of past events that may be helpful in explaining the present or anticipating events."

Being able to interpret perspectives from various documents and personal accounts gives benefit to historical research. Since it deals with the meaning of events, the heart of the historical method is not only the accumulation of facts, but also the interpretation of the facts (Leedy, 2001). The focus of this historical research will be to trace the evolution of information assurance initiatives. The intent will be to identify programs and initiatives developed to assist with the protection and defense of information and information systems during military operations. The purpose will be to identify specific aspects still present or those that have changed with technology and time.

I will develop of an overall evolutionary model based on factors that relate to information assurance, information operations, information warfare, and current and past military operations. Additionally, I will parallel related factors with information that supports the validity or lack thereof by other historical documentation on this subject.

Scope and Limitations

The overall focus of this research effort will center on the historical perspective of information assurance during military operations and the critical time between conflicts and the identification of potential doctrinal changes. This research effort will focus on the U.S. Military during various operations since WWI through Vietnam related to IA in its current form. Limiting this effort to this period and concepts will narrow the overall analytical scope and provide a snapshot into a specific time when electronic and communication advancements began to enhance the technological competence of the warfighter. This research will focus on documentation that explores Command, Control, Communications, computers and Intelligence (C4I); military leadership; decision-making

processes; and defensive measures that concentrate on the protection of information and information system resources.

Significance

Advancements in technology and innovation continue to produce constant change in military environments. These advancements also provide a clear understanding of concepts that aid certain evolutional aspects over time. This research is intended to assist in the understanding of the evolving role of IA in the U.S. Military.

Thesis Overview

Chapter One included a brief overview of the background information, a description of the overall methodology, presentation of the research questions, and the intended significance of this research effort. Chapter Two reviews the research methodology and overall theory and provides justification for using various historical approaches and IA models. Chapter Three explores current literature on the historical perspectives of warfare and the protection of information and summarizes background information pertinent to Information Operations (IO) strategies related to aspects of Defensive Counter Information (DCI) under the IA domain. Chapter Four discusses the findings from an analysis of the information presented in Chapter Three including research questions one and two. Finally, Chapter Five provides a discussion of research question three, limitations, suggestions for future research, and conclusions.

II. Methodology

Introduction

Chapter One provided background information, described the research problem, and briefly discussed the research scope and methodology. This chapter will describe the methodology used to investigate the research problem and theory proposed in chapter one. This chapter will also provide justification for using the historical research method for Management Information Systems (MIS), the National Security Agency's Information Assurance Model (IAM), and the Information Assurance Model presented by McCumber and Maconachy et al.

Research Methodology

A historical research methodology was chosen for this thesis effort. Historical research is defined as a systematic process designed to collect and objectively evaluate data related to past occurrences to arrive at conclusions that may be helpful in explaining the present (Nel, 1983). Historical research also uses inductive reasoning approaches to build theories that ultimately draw conclusions about entire classes of events. Leedy et al (2001) describes historical research as separate and individual facts observed by the researcher and used to assist with the establishment of a specific theory. The goal of this research effort is to build theory by using a specific framework and interpreting the information and facts presented. Since historical research involves independent investigation, it is important to ensure that common problems do not plaque this effort. Borg et al (2002) discusses two common problems with historical research. First, it is

difficult to maintain rigor or avoid external criticism of the use of non-authentic sources. Secondly, maintaining objectivity or avoiding the biases and distortions that define internal criticism can lead to additional problems. Reflecting on the purposes of history as a mirror, the French philosopher Michel Foucalt commented:

> "The final trait of effective history is it's affirmation of knowledge as perspective. Historians take unusual pains to erase the elements of their work which reveal their grounding in a particular time and space, their preferences in a controversy – the unavoidable obstacles of their passion."

In Paul Godfrey's (1996) assessment of Mr. Foucalt's assessment he states:

> "Foucalt's evaluation of history demonstrates that any treatise that goes beyond the mere recitation of chronological events, speaks more about the researcher's own intellectual, moral, and emotional location than about a "correct" evaluation of historical events. The task must focus on revealing the mirror through which history is viewed as well as history itself."

In other words, it is important to present to others historical facts that are grounded by credible sources and thorough interpretation of the pertinent details of the specific topics covered.

To alleviate the risk associated with the problems identified above, the specific methodological approach must demonstrate objectivity and accuracy. To ensure these concepts, several libraries were searched for information dealing with IA during past military conflicts. Initially, the Air Force Institute of Technology (AFIT) along with Wright State University and the University of Dayton, all of which are located in Dayton, Ohio, were used as primary research facilities. Follow on research conducted at Marine Corps University (MCU), Quantico, Virginia provided an extensive amount of resources related to communications and intelligence during past military conflicts. MCU was also a first rate location and facility for any material related to the history of warfare.

Approach

A historical research approach in MIS developed by academics working on a research project at Harvard University's School of Business provides structure and purpose for this current effort. McKenny et al (1997) developed a seven-step methodology for conducting historical research in MIS. This seven-step process, modified to meet the current requirements, provides a specific structure and an overall outline to the period being researched and the presentation of information discovered:

- Begin with focusing questions.
- Specify the domain.
- Tell the story
- Write the transcript
- Gather the evidence
- Critique the evidence
- Determine patterns.

This seven-step process helps to establish the specific format needed to view pertinent information used to analyze present circumstances throughout the MIS field. The steps identified will also lead the researcher and research towards the development of a robust MIS historical research theory.

Current IA theory identified in chapter one discusses the five building blocks for any successful IA program; availability, integrity, identification, confidentiality, and non-repudiation (JP 3-13, 1998). As the current IA theory focuses on these building blocks, it is important to demonstrate where this information fits into the historical domain.

Theories developed by McKenny et al (1997) support these building blocks by demonstrating how history and historical research provides a backdrop from which to determine what is novel in any current situation and which factors serve to distinguish the present from developments of the past. Stanford (1986) describes the structure of historical research as follows:

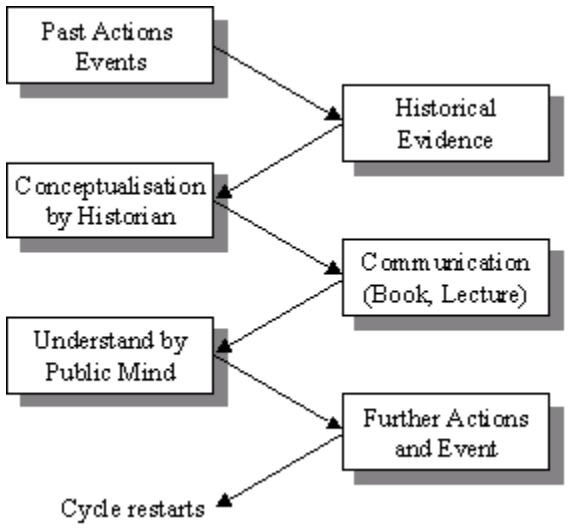

Figure 2: Structure of History (Stanford, 1986)

Bannister (2002) describes the Stanford model as significant in the interpretive processes encountered from historical research, over a long period of time, when the researcher may not have been present.

In a study of Bank of America and it's banking operations achievements, the researchers developed the concept of the Dominant Design. A dominant design is a design that has the potential to yield superior results for any organization. It is generally a result of a radical – as opposed to an evolutionary – innovation in an industry. Even though the concept of the dominant design is a result of a radical and not an evolutionary

innovation, there is indication throughout the history of U.S. wartime operations that dominant design often took place. As events happened, various processes turned into evolutionary events over time and ultimately shaped the outcome of current events. McKenny et al (1997) also proposed a framework for information systems research during the Bank of America study. This framework provides a distinct concept that further demonstrates the realization of dominant design within the organization. This concept is the cascade approach. The cascade approach is a conceptual framework for describing the development or emergence of an information system. The following key areas make up cascade process approach:

- Crisis.
- Search for a technical solution.
- Initial technical solution found.
- Adjustments throughout the organization.
- Assets formed, which resolves crisis.
- Dominant Design.

The basis for this framework is developed on the notion that there is a crisis within an organization, which is resolved by the use of information technology or system (Bannister, 2002). The crisis within the scope of this research is war or conflict of the U.S. military since WWI. Within the realm of the protection of key communications, major crisis, followed by concepts identified in the cascade approach, shaped the tactical nature of how various communications activities developed and ultimately changed with advancements in technology. Bannister (2002) also believes that successful completion of the cascade process relies on the three roles of the leader, maestro, and super-tech to

drive the organization towards the overall goal of the dominant design. Evidence suggests that events related to MIS and IA during past military conflicts have followed similar paths towards the creation of new techniques and procedures.

The National Security Agency's (NSA) Information Security Assessment Model (IAM) identifies 18 baseline categories that should be included as components of the Information Assurance posture of any organization (Hurd, 2001):

Table 1: NAS IAM 18 Baseline Categories (Hurd, 2001)

1	IA Documentation
2	IA Roles and Responsibilities
3	Identification & Authentication
4	Account Management
5	Session controls
6	External Connectivity
7	Telecommunications
8	Auditing
9	Virus Protection
10	Contingency Planning
11	Maintenance
12	Configuration Management
13	Back-Ups
14	Labeling
15	Media Sanitization/Disposal
16	Physical Environment
17	Personnel Security
18	Training and Awareness

These categories are generally accepted when developing and maintaining systems under the information technology (IT) realm (Swanson, 1996). Even though there are several organizations that provide justification of important categories, the NSA IAM was developed specifically for government and commercial organizations and is often

referred to as the accepted standard for IA related system certifications to enhance the protection of information and the establishment of functional IA programs (Hurd, 2001; 256).

A limited number of models dedicated to the understanding of threats to automated information systems are currently available. The McCumber (1998) model is used to appropriately organize the 18 baseline categories for analysis and to address the possible threats to automated systems. This comprehensive model addresses threats and functions as an assessment and evaluation tool. McCumber argues that it is a key concept because it is independent of technology and is not constrained by organizational differences and thus can be used for systems development. The three dimensions focus on information states, critical information characteristics, and security countermeasures. Maconachy et al (2001) expanded the McCumber model to include the theory that we are now in an information intensive environment, which broadens the scope and the overall understanding of information and systems protection. The strength of the multidisciplinary and multidimensional elements of the McCumber model is in its ability to produce or maintain a robust IA program. Figure 2.3 shows this model and demonstrates an integrated approach that accounts for three of the four dimensions of IA, information states, security services, and security countermeasures.

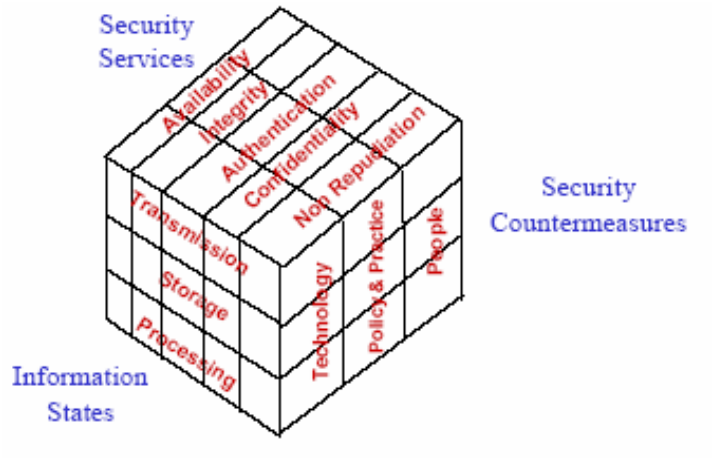

Figure 3: Information Assurance Model (Maconachy et al, 2001)

Additionally, Maconachy et al created a fourth dimension, time. The time dimension of the integrated model demonstrates the introduction of new technology over time requires modifications to other dimensions of the integrated model in order to restore a system to a secure state of operation. This dimension is related to the notion that certain aspects of the McCumber model has changed with innovation and is essential to the theory that IA throughout military operations in warfare has evolved from earlier concepts. Essential elemental changes over time were fundamental to the adoption of new technology or doctrinal enhancements that were evident during military conflicts. Such changes to the system over time were key aspects of restoring a secure state.

Using a current framework such as the Maconachy et al (2001) model to evaluate past occurrences will provide evidence about whether the concept currently known as IA is valid for earlier U.S. Military conflicts. A modified list of the baseline categories are grouped in Table 1 below using the Maconachy (2001) model. This grouping will form

the foundation for the evolutionary model that will be developed further in this research effort.

Table 2: IA Model - NSA IAM Mapping

IA Model Dimensions	NSA IAM Baseline Categories
Information States	
Transmission	External Connectivity
Storage	Back-Ups Disposal
Processing	Auditing Session Controls
Security Counter Measures	
Technology	Maintenance Telecommunications Virus Protection
Policies and Practices	Account Management Configuration Management Contingency Planning IA Documentation IA Roles & Responsibilities Media Sanitization
People	Awareness Personnel Security Physical Security Training

Each category has specific questions or pertinent information that should be included when conducting an IA assessment and will demonstrate the applicability of earlier indicators relating to information and information systems protection during the various military conflicts since WWI. Accordingly, significant principles collected and organized into two of the four dimensions of the IA Model will be depicted here. The information states and security countermeasures dimensions will form core data elements

and demonstrate the applicability of earlier concepts relating to the security of information WWI through Vietnam with the present structure of IA.

Justification for Historical Research Method

Mason (1997) identifies four products that can result from a MIS historical research focus:

- An account of significant fragment of the past describing events of importance to the MIS community. The account in and of itself is informative, but also serves as contextual material for understanding other events.
- The resulting historical account may be used subsequently as a "datum" in a broad process of inductive reasoning.
- Historical research may serve as the source of new research hypotheses.
- Historical research results in a better understanding of the present with indicators that will assist in meeting related future requirements.

Current technological advancements throughout the IA field have stemmed from significant events of the past. Research that demonstrates how IA has evolved into its current structure will fit into any category identified above. The products of historical research are abundant throughout the IS community even though Bannister (2002) believes there remains a distinct shortage of good MIS or IS historical studies of information systems in organizations and how these systems influence and shape organizations over time. The theory is that the study of IS using historical perspectives is still in its infancy. Over the past 30 years, the focus tends to be either on the history of specific technologies, technology companies, or the impact of developments on an industry (Bannister, 2002).

The primary intent of this research effort is to produce an initial working model to demonstrate a historical perspective on the IA aspect of IS. This model can also provide IA professionals with the support of future initiatives or innovations. A review of existing literature will attempt to disclose information concerning a model that focused on the evolution of IA before 1960. While there is some theory of IA and information system security structures, no current framework focuses on the evolutionary process prior to 1960. This will be accomplished by the systematic research effort outlined and supported by research questions discussed in chapter.

Chapter Review

This chapter discussed the detailed methodology used to investigate the research problem and the proposed theory. This chapter also provided justification for the historical research method for Management Information Systems (MIS), the National Security Agency's Information Assurance Methodology (IAM) and the McCumber and Maconachy model of Information Assurance.

III. Background

Introduction

The previous chapter described the detailed methodology used to investigate the research problem and theory proposed in chapter one. Additionally, the previous chapter provided justification for using the historical research method for Management Information Systems (MIS) and the National Security Agency's Information Assurance Model (IAM). This chapter explores current literature on the historical perspectives of warfare and the protection of information from World War I through Vietnam to the present. This chapter also summarizes background information pertinent to Information Operations (IO) strategies related to aspects of Defensive Counter Information and the Information Assurance (IA) domain.

Early History

Before focusing on the current period, I will first explore how early warfare relied on various methods of protection of pertinent information from the enemy. Exploring the background of security schemes developed during early warfare will provide a foundation for discussing American Military warfare from WWI through Vietnam to the present.

Field Marshall Bernard Law Montgomery, a British Military commander during World War II, described the information security requirement:

> "A good military leader must dominate the events which encompass him; once events get the better of him he will lose the confidence of his men, and when that happens he ceases to be of value as a leader. He has therefore got to anticipate enemy reactions to his own moves, and to take

> steps to prevent enemy interference with his own plans" (Montgomery, 1968: 16).

While Montgomery's statement demonstrates the power of combat leadership, the protection of key information helps combat leaders gain significant advantage over enemies. The domination of events during warfare facilitates the primary goal of IA, to protect and defend information and information systems (JP3-13, 1998). Confidentiality is maintained when information relevant to combat plans is safeguarded from enemy commanders. Throughout the history of the world, records demonstrate how military commanders have always wanted to safeguard information related to operational strategies and actions to prevent enemy interference with tactics. At Jericho in 7000 B.C., precautions taken to fortify the city included walls and moats to keep the enemy out (Montgomery, 1968: 29). These fortifications allowed only enemy speculation of what was within those walls. Other early methods of safeguarding information came in the form of torches used for signaling movements; trusted runners used to relay important messages to commanders; and trumpets or other instruments used to relay battle commands to soldiers (Montgomery, 1968: 39).

The Arab raiders of early medieval warfare used the element of surprise to gain advantage over villagers by overwhelming them before they were fully aware of what was happening (Montgomery, 1968: 145). The element of surprise used by the Arabs ensured they had an advantage over the people of the countryside. Such actions protected pertinent battle information until it was too late for a counter attack. The Greeks made great strides in cryptography, which is recognized as one of the earliest forms of confidentiality or maintaining privacy of sent messages. They used fires and torches to

send messages representing letters of the Greek alphabet. Other forms of cryptography included shaving the heads of slaves, writing messages and concealing the message by letting the hair grow back. Once the hair returned, the slave was sent to deliver the message (Churchhouse, 2002). Another method involved the Greek scytale. The scytale is a wooden pole used as a transposition cipher by the Spartan military. The sender would write the message along the length of the scytale on a strip of leather or parchment, and then unwind the strip, which would appear to carry meaningless letters. A person with a staff of the same size, often fabricated at the same place, would be the only person able to read the message (Newton, 1998). Such techniques provided key operational instructions and advanced warnings to commanders in the field. Fires and torches also provided ways to assist battle ships navigating the Greek shoals (Wrixon, 1998).

At the height of the Roman Empire, Julius Caesar used a combination of signaling stations and various ciphers to communicate with his generals. Caesar is known as one of the first persons to have ever employed encryption for the sake of securing messages during warfare (Morelli, 2002). The Caesar cipher was used by Julius Cesar to communicate with his armies using Greek letters to mask Latin messages (Wrixon, 1998; 170). This encryption procedure used shifting techniques of the normal alphabet in plaintext to code messages that were later decoded using a cipher text. The cipher text identifies the actual alphabet substitution technique (Bosworth, 1982). The techniques used by leaders of the great Arab, Roman, and Greek Empires were all aimed at protecting the uninterrupted flow of information, which is a key aspect of IA. These early examples demonstrate how the true origins of IA are associated with the most

primitive forms of warfare. They also reveal how the concept of IA has evolved over time from initiatives and strategic actions taken, which led to military leaders focusing on the best ways to gain advantage over adversaries.

The New World

The Industrial Revolution, which started in Europe and progressed to the new world, brought great advancements in weapons, armor, and communications. A major advancement in communications came in the form of the telegraph. Samuel Morse invented the telegraph in 1832 (Montgomery, 1968: 420). The telegraph provided a primary means of communication during the American Civil War. The telegraph also provided an early electronic system that helped with the advancement of military communications. "Although telegraph messages were frequently sent in code, the recipients were relying on the integrity of the telegraph companies than on the codes for security" (Diffie, 2003). Even though the early telegraphic systems were not developed to protect sent messages, many devices developed automated the message process. Since the telegraph was a primary means of communication, both the Union and Confederate Armies tapped lines. In his book, *The Secret War for the Union*, Edwin C. Fishel stated that even though the telegraph had the potential to yield great intelligence, there are records that indicate tapped lines yielded no pertinent information that could be used by either side (Fishel, 1996: 4).

During the American Civil War, intelligence collection obtained by the signal corps became a primary means of obtaining enemy information. Opposing signal corps would collect intelligence by observing troop movements using signal towers, rooftops,

and hilltops. Counter measures by both sides often relied on the minimal use of flags, which would pinpoint their location or other key operational information (Fishel,1996: 5). Such tactics also demonstrate how confidentiality and the protection of sent messages was the main reason for the development of certain defensive strategies during the Civil War.

World War I

The military importance of the radio and advancements in communication technology influenced key decisions in the United States Government during WWI. On April 7, 1917, all amateur and commercial use of radio came to an abrupt halt as the United Stated entered into WWI. Radio stations were ordered to shut down or were taken over by the government. This precautionary measure taken by the United States helped to ease the growing concern of an ill-prepared U.S. Military to cope with the communication needs generated by entrance into the war (De Gallaix, 1919). Emergency measures adopted during the early stages of the U.S. involvement suggest there were no alternative message systems available prior to this time. According to Diffie (2003), "the military radio in wartime was so valuable that no one could completely forgo its use." However, the problem with the radio was its simple use. From a security standpoint, it was easy to send and receive transmissions. In order to protect radio transmissions, military leaders incorporated the use of cryptography as a security measure (Diffie, 2003). According to *The History of Codes and Ciphers in the United States during WWI,* four additional factors led to the increased use of codes and ciphers for wartime communications (Barker, 1979; 126):

- The increasing use of wire communications increased the demand for encryption methods to prevent enemy access.
- The invention of the steam and gas engine provided greater mobility of military tactics and increased the need for encryption methods for communications.
- The invention of the radio and its speedy adoption for military use.
- The invention and development of the aircraft and the speedy adaptation for military operations.

One major communications function during WWI focused on maintaining the confidentiality of sent messages, which is the fundamental objective of cryptography. This objective also has other important applications that focus on the authentication of messages and the protection of sent data (Soergel, 2002). Such techniques rely on the notion that there is a message; however, it is difficult for unauthorized persons to read or understand it (Joyce, 2002). Another essential element used in cryptography is encryption. Encryption is the process to encode a message so that the contents are hidden to unauthorized individuals (Soergel, 2002). This encoding process is essential to allow a message to be un-readable by unauthorized persons. Cryptographic systems also use ciphers and cipher devices. The word cipher is Arabic for "nothing" and is a method of concealment in which the primary unit, letters of a particular alphabet, are substituted with other letters, numbers, or symbols. A cipher device is a manual mechanism used to encrypt and decrypt messages. A cipher is also method of concealing or keeping secret the meaning of a word, phrase, sentence, or longer message in which the basic unit of concealment is the letter (Newton, 1997; Wrixon, 1998).

The greater need for secure communications became apparent when the American Expeditionary Force (AEF) first arrived in Europe. The AEF's radio, telephone, and courier dispatches urgently needed encryption protection (Wrixon, 1998). There were three cryptographic systems used during high-level communications by the U.S. Army. *The War Department Telegraph Code 1915*, *The Army Cipher Disk*, and *The Playfair Cipher* were used throughout the early stages of the war despite the notion that they were believed to be insecure and unreliable. However, only the *War Department Telegraph Code 1915* and the *The Playfair Cipher* were used in Europe (Barker, 1979; 126-127). Since secure communications by encryption was essential to the U.S. Military, leaders began to focus on the development of other forms of encrypted communication. This led to the development of several experimental codes by the Code Compilation Sections in Washington and France that were evaluated by the Military Intelligence branch of the War Department known as MI-8 (Barker, 1979; 33; Wrixon, 1998). The evaluation of the various codes led to the development of two-part codes, which were more complicated and provided greater levels of security. Even though the AEF had limited knowledge of cryptographic techniques at the beginning of the American entrance into WWI, by late 1918 the U.S. had made significant strides in ciphers and encipherment methods.

During the closing days of WWI, eight Choctaw Indians emerged as key communication specialists to the AEF. During the Mousse-Argonne campaign, the Choctaw "code talkers" used their native language to encode key information over open radio channels. Other native Choctaw speakers decoded the messages and conveyed the information to AEF company commanders. Over the course of a few weeks, they

handled field telephone calls, translated radio messages, and wrote field orders. German eavesdroppers who had tapped radio and telephone lines and broken American radio codes could not interpret the Choctaw language (Green, 1979; Wrixon, 1998; 357).

The successful use of the radio throughout WWI allowed communications between military units who were considerable distances apart. However, transmission techniques were also vulnerable to interception by the enemy (Churchhouse, 2002; 111). Many countries realized that the use of encryption techniques to encipher and decipher messages could be used for secure communications in future military operations. Consequently, several developments would shape the future of military secure communications techniques.

During the 1920's, one of the most famous crypto graphical machines, Enigma, was invented by Arthur Scherbius, co-founder of a German engineering firm (Churchhouse, 2002; 111). Prior to Enigma, there were a number of methods used to encipher messages. Such methods were based on the use of books of numerals held only by the sender and the recipient. Each service had its own particular code book with a multitude of words and phrases likely to be used by a particular service. There were opposite phrases and words in each numerical group (Winterbothan, 1974; 8) The original Enigma was constructed and shown in Vienna in 1923, however, the machine was not adopted for military use until Adolph Hitler began to rearm Germany during the late 1920's. The German High Command (GHC), with counsel from German cryptographic experts, decided that Enigma offered satisfactory guarantees of security after several modifications and improvements (Kahn, 1968). The GHC considered the Enigma machine top-secret and the code unbreakable even though the original machine

was shown to the public. The GHC eventually equipped all branches of the German armed forces with the device (Dziewanowski, 2001: Churchhouse, 2002; 132: Haufler, 1999).

The Hagelin cipher machine was another important cipher of the late 1920's. It was developed by Boris Hagelin and manufactured in Sweden. The Hagelin cipher could print and provided greater accuracy than the Enigma machine. It was marketed to any country and was eventually purchased by Germany, Italy, the United Kingdom, the United States, and France under a variety of names including the M209, C36, C38, and C41 (Churchhouse, 2002; 133). By 1942 and continuing into the 1950s, improvements to the Hagelin machine were initiated by the American, French, and Italian militaries. The machine was modified for improved performance, reduced in size, and mass produced to support individual war efforts by each country (Kahn, 1968; 426-427).

According to Polish intelligence accounts during the early stages of WWII, counterintelligence agents intercepted an Enigma machine dispatched from Berlin to the German legation in Warsaw in 1929. Three years passed before Polish scholars could break the secret to the German cipher. By 1939 and on the eve of the war, the polish intelligence service could decode most German messages. After this accomplishment, the Polish made replicas of Enigma available to allied commanders. They furnished machines to French and British intelligence officers (Dziewanowski, 2001). Obtaining and breaking the German cipher would prove significant since the world was on the brink of the Second World War.

World War II

The success of the Choctaw code talkers during WWI prompted key military leaders to find additional Native Indian speakers for tactical combat communications during the early stages of World War II (WWII). Twenty-five years earlier, there were only eight Choctaw code talkers during WWI. The Choctaw code talkers were instrumental in the establishment of other military units composed of other Native Indian speakers serving as communications specialists. The U.S. Army formed a communication unit that consisted of seventeen Comanche assigned to the Comanche Signal Corps of the Army. Like the Choctaws before them, they handled field telephone calls, translated of radio messages, and used their language with a combination of specialty crafted military terms to write field orders for radio transmission that could not be understood by the Germans (Wilson, 1997). Several tribes spoke across enemy lines in Africa, Sicily and the South Pacific. During 1939 to 1945, the Army tapped Hopi, Choctaw, Comanche, Kiowa, Winnebago, Seminole, Navajo and Cherokee Americans to use their languages to communicate. Even though such techniques were considered secret codes, the Indian tribes were only using their native dialects and not actual codes (Dorn, 1973).

The most recognized of the code talkers were the Navajo. The Army continued to use Native Indian speakers to encode and decode vital battle information. However, the Marine Corps devised a different technique to employ unique Native Indian languages as secret codes during WWII. During the early stages of WWII, the Japanese cryptographers had become very efficient at breaking top-secret military codes. Philip Johnston, who had served with U.S. forces in France and had lived on a Navajo

reservation as a youth, was convinced the Navajo language could be used a secret code against Japanese cryptographers (Molnar, 1997; Wilson, 1997). According to Carl Gorman, one of the original code talkers, "the language was unwritten at the time and was based solely on the sounds, which made it difficult for others to understand (Bandrapalli, 1997)." Philip Johnston eventually convinced key Marine Corps leaders of the potential of the Navajo language. The Navajos were the only Native American Tribe recruited specifically to be communications specialists. Over 400 Navajos completed Marine Corps boot camp and wartime training at Camp Pendleton's code talker school. The Navajos developed a technique that used native words translated into common warfare or battle terms (Dorn, 1973; 7). Most were assigned to combat units overseas and the Commandant of the Marine Corps (CMC) recommended that a crew of qualified "talkers" be assigned to each Marine Corps Division and the remaining "talkers" to a training center in the South Pacific (Dorn, 1973; 60). Eventually the code became the main method of secret radio communications during pivotal battles in the pacific (Bandrapalli, 1997; Wilson, 1997). A staff writer for the Marine Corps Magazine, *The Leatherneck*, commented on the code talkers:

> "Voice Code transmission of operational orders laid the groundwork from the Solomans straight through Okinawa" (Dorn, 1973; 57).

It is clear the effort and dedication of the code talkers made significant impacts on the pacific operations of the war. In an interview, Major Howard Conner, the Fifth Division's Signal Officer, described how the Navajo code talkers performed during the Iwo Jima landing:

> "The entire operation was directed by the Navajo code….During the two days that followed the initial landings I had six Navajo radio nets working

> around the clock…They sent and received over 800 messages without error. Were it not for the Navajo Code Talkers, the Marines never would have taken Iwo Jima" (Wilson, 1997).

The use of the Navajo code became one method of U.S. secret radio communications during key battles throughout the pacific theater and was often referred to as "the code the Japanese couldn't crack." The unique relationship between the Navy and the Marine Corps allowed Navajos based on ships or shore to communicate with each other quickly and accurately and prevented the enemy from acquiring early knowledge of future events (Dorn, 1973; 58; Bandrapalli, 1997).

In addition to the Navajo communicators' ability to transmit secure messages, there were other significant efforts aimed at secure communications technology. The A-3 scrambler system operated by the American Telegraph and Telephone (AT&T) Company was considered state of the art technology during WWI, however, during the early stages of WWII, it was vulnerable to anyone with sophisticated unscrambling capability (Boone et al, 2000; Weadon, 2000). In an effort to control persistent communication problems, the U.S. and its allies set out to develop a means to protect their information. Bell Telephone Laboratories, under the direction of A.B. Clark with assistance from British mathematician, Alan Turing began to work on "the Green Hornet" which was later referred to as SIGSALY (Boone et al, 2000; Weadon, 2000). SIGSALY provided "pulse code modulation", which is known as the predecessor of present-day innovations as digital voice, data, and video transmission. Additionally, early applications of spread spectrum technology were developed. SIGSALY is a device that helped to provide a springboard into the digital communication world. Formal deployment began and provided a great advantage to the U.S. and allies in July 1943 because of its ability to

offer truly secure voice communications at high organizational levels (Boone et al, 2000; Weadon, 2000).

The resourcefulness of the allied forces to intercept and decode key communications by the German and Japanese diplomatic and military leadership also proved vital to the allied war effort. According to the National Security Agency's *Korean War Background of Signals Intelligence* (SIGINT), cryptanalytic units expanded and close ties between the U.S. and Great Britain at the outbreak of WWII facilitated their efforts. Military and civilian decision makers obtained detailed inside information about the enemy. The enhanced activity paid off in plentiful and high-quality information on the Germans and Japanese – their location, armament, and intentions (Hatch, 2000). During early stages of WWII, the Germans and Japanese were using various adaptations of Enigma for key communications. Enigma was used to control and report locations of submarines in the Atlantic and to pass information about bombing raids, the movement of military units, and the location and cargo of military supply ships (Adamy, 2003). Unknown to the Germans, their secret communications weapon had been compromised long before the war began. The Polish success in breaking the secrets to Enigma and subsequently using the machine to decode German messages would be vital to allied military operations for American, British and French forces. After an arrangement between the British and Polish government, the sharing of the Enigma and relevant intelligence was turned over to the British. The British improved the techniques developed by the polish at the Government and Cipher School at Bletchley Park, United Kingdom. The Ultra Secret Intelligence Agency, or "Ultra", was the result of British improvements to Polish methods of deciphering at Bletchley Park. This technology was

later turned over to the American government, who also assigned American military personnel to Bletchley Park to work on the "Ultra Secret" (Dziewanowski, 2001; Haufler, 1999).

Another major contributor to the code breaking effort of German military communications was Bombes. Designed to replace several time consuming manual methods used for the heavy amount of Enigma intercepts, a series of machines known as Bombes were created to look for certain sequences of characters and comparisons of various Enigma settings (Lee, 2000). Although the British originally manufactured Bombes in Europe, the U.S. Navy led the effort to manufacture enhanced Bombes in the U.S. to combat the growing concern for the German U-Boat codes used to coordinate attacks on U.S. ships in the Atlantic. The National Cash Register (NCR) Company in Dayton, Ohio was awarded the contract to manufacture Bombes. The U.S. Bombes were far superior to previous versions and allowed cryptologists at Bletchley Park to focus on the production of other code breaking requirements (Lee, 2000).

Even though the information presented above concentrated on the breaking of German codes and devices center on offensive tactics, it demonstrated the German lack of effective information and information security practices. The German failure to practice procedures that led to a greater focus on the security of communications functions would ultimately lead to allied progress towards victory in the Atlantic and Pacific. The efforts made by the U.S. and Great Britain to intercept and break German codes would also prove to be decisive to the overall strength of allied militaries.

The National Security Agency's *Korean War commemoration on signals intelligence (SIGINT)* summarized that by the closing days of WWII, military personnel

wanted to return to their homes and consequently a large number of personnel left cryptology for civilian life (Frahm, 2000). From 1945 until the start of the Korean War, President Truman slashed the military budget in an effort to reduce the deficit created by the war. Additionally, only the most critical cryptology positions were filled due to deficit reduction efforts and other, more important, U.S. commitments. Communication efforts focused on the Soviet Union, which stemmed from increased tensions of the cold war and the fall of China to the communists. As a result, there were major structural and doctrinal changes associated with military communications (Frahm, 2000). In 1949, all three military cryptologic services were centralized under the new Armed Forces Security Agency (AFSA). In addition, the Army Security Agency (ASA) and the Air Force Security Service (AFSS) also played important roles to the overall communications posture of the pre Korea timeframe (Weadon, 2000).

Korea

On June 25, 1950, in an effort to reunify the Korean peninsula under communist rule, the North Koreans launched a massive offensive led by 150 soviet tanks against South Korea. Within days, the Capital of Seoul was captured and there was a steady push further south (Frahm, 2000). Prior to the North Korean offensive, the U.S. Government characterized Korean communication activities as a low-level priority. Intercept activities and limited cryptographic support in the region centered on the monitoring of Soviet and Chinese communist activities. Even though there were several intercepts prior to the beginning of the war, coverage was dropped once analysts confirmed the non-Soviet origin of the material. Major efforts focused on Communications Intelligence

(COMINT) which centered on the ability of U.S. Forces to conduct communications intercept activities in support potential offensive operations (Hatch, 2000: Johnson, 2000; 39). According to an assessment of the Korean War conducted by Thomas Johnson (2000), "the Korean War occurred during a period of struggle in the cryptographic community. It began a year after the formation of the AFSA and concluded after the AFSA ship had been scuttled in favor of a new vessel, the National Security Agency."

As with WWI and WWII, the U.S. was ill prepared to cope with many of the communications challenges faced during the early stages of the Korean War. In fact, even though WWII had concluded five years earlier, various stages of the war in Korea produced a resurrection of WWII communication standards, guidelines, and common practices, including American strategic level communications (Hatch, 2000). The dependable SIGABA device, developed from the earlier SIGSALY device, and tools such as the M-209, secure communications continued to keep American plans and intentions from the enemy. Many believe that the SIGABA was the most secure cryptosystem of its era and that no SIGABA traffic or battlefield communications were read during the latter stages of WWII or Korea (Diffie, 2003; Weadon, 2000).
Most of the U.S. communications strategies focused on maintaining a steady flow of enemy intelligence and security concerns aimed at protection of information and personnel. In personal interviews conducted by John G. Westover with members of the United States Army who served during the Korean conflict, there is a clear indication that certain factors contributed to the security of information. Many of these factors relate to the four dimensions of IA; information states, information characteristics, security

countermeasures, and time discussed earlier. Several of these personal accounts are provided below (Westover, 1987; 87-106):

- *LtCol. George Lieberberg, Signal Section, HQ Eighth Army.* "Since there was no anticipation of this war and the U.S. priorities were concentrated elsewhere, military personnel staffing to the region was a major concern. The first order was to dispatch troops with communications specialties from Japanese region to the Korean."

- *Capt. John W. Pierce, 24th Signal Company.* "Although wire is the primary method of signal communications, in Korea we had to use very high frequency (VHF) radio because distance, speed, terrain, and road nets limited the use of wire." "The isolation of the VHF terminals was a major concern….The isolation of the U.S Forces also brought a serious security problem. With no headquarters personnel nearby to provide security, we sometimes requested help from the Korean National Police. I did not have much faith in the personnel of this force, and in some cases it was better to use our signalmen as guards."

- *Capt. Frank D. Secan, 304th Signal Operation Battalion.* "In teaching about VHF radio, instructors often place more emphasis on the difficulties of line-of-sight than is necessary. VHF waves bend, bounce, and do many other tricks. I have aimed such waves up valleys, through mountain passes, and once directed my beam directly at a large mountain – yet had the signal clearly received." "I have seen a number of VHF stations located on the crests of hills and mountains to take advantage of line-of-sight. On the slope you can get out of the wind, with its consequent technical troubles and personal discomforts much easier."

- *Capt. Wayne A. Striley, 71st Signal Service Battalion.* "The destruction of signal equipment was greater in Korea that in WWII." "The key cable used for Korea's telephone-telegraph system was in pretty bad condition from bomb explosions, artillery, and mortar fire."

- *SFC Richard L. Albrecht, Headquarters, 24th Division Artillery.* "In their enthusiasm to get messages delivered, a number of message centers sent communications by several methods. All classified messages – even those labeled Restricted – had to be encoded before they could be transmitted by radio. It always

seemed we got our coded messages at night. It was normal most evenings fo the code clerk to work several hours on messages, only to find that the same messages had already been received by courier and distributed."

- *Lt. Arthur J. Cramer, 7th Signal Company.* "The entire cryptography system is cumbersome under the best conditions, but it is intolerable when it is not working properly. Typical of the conditions that slow up the system were the over-classified messages. We received so many five day old Flash (highest priority) messages from X corps that they became a joke." "Our cryptographers were overburdened with long messages that were also forwarded by some other (and often faster) method. Many times at night I would awaken my whole crew to get them working on a number of long messages – only to find they had previously been received by telephone in the clear, or had been brought by courier."

- *From Signal, November-December 1951.* "Carrying messages by plane is nothing new, but in Korea it has become important. Jeep, or motor messenger service, had always received more use until the Korean campaign made getting messages from one battlefield to another more difficult." "The airplane performs an important job which is as old as warfare: getting the message through." "The answer to the bad roads was the light airplane, the L-5, or "mosquito"."

As acknowledged in the personal accounts above, U.S. forces persevered under extreme conditions to ensure the protection of information and information systems during the Korean War. Key concepts of these personal accounts demonstrate how poor staffing, difficult and unfamiliar terrain, redundant practices, inexperience, and various other factors led to innovations and practices that evolved into vital concepts that align with the four dimensions of IA discussed by Maconachy (2001).

Another factor that affected the security of information was press releases that provided too much information on the exploitation of enemy communications. To limit such activities, military leadership implemented drastic measures such as suspending

COMINT operational support to battlefield commanders until key security concerns were alleviated (Johnson, 2000: 56).

COMSEC during the Korean War demonstrated a fluid tactical situation during the early stages of the fighting. This led to the destruction of high-level machine ciphers to prevent their capture (Finnegan, 1998: 114). Other COMSEC vulnerabilities centered on the general lack of a vigilance and awareness by service members, which increased the number of security violations. These violations were normally taken lightly due to more important problems like the general speed and availability of communications for the war fighter (Finnegan, 1998; 150).

The closing stages of the Korean war saw changes in national security policies and overall defensive management structures that aligned with the new Presidential administration and a general dissatisfaction of the American public. This dilemma centered on recently ended fighting with the signing of the Korean armistice in 1953. As with the previous wars, military personnel levels were reduced in favor of "lean" forces. Additionally, the concentration on warfighting capabilities that included tactical nuclear weapons led to various revamping strategies focusing on the Soviet threat (Fennigan, 1998: 122).

Other developments during the 1950s included the Army Security Agency's (ASA) awareness of possible security concerns stemming from emissions of electronic data processing equipment. The ASA initiated a program named TEMPEST. The function of TEMPEST related concepts center on compromising emanations generated by electromagnetic radiation, which interferes with radiation and could possibly leak information about the data being processed on an unprotected machine (Kuhn, 1998). To

counter the threat posed by TEMPEST and other security concerns, the ASA formed boards to provide long range planning and research into programs that would counter the threat to electronic data processing equipment that might compromise security (Fennigan, 1988; 129).

Vietnam

As with previous wars, the period leading up to the Vietnam War provided the opportunity of the American leadership to establish programs that would focus on restructuring and reallocating personnel and resources to other, more important missions (Fennigan, 1998: 121). During the early stages of the Vietnam War, ASA companies provided communications support for tactical units throughout Vietnam. Initially, such practices were aligned with police type functions of monitoring friendly communications and warning of possible compromises. Many military personnel also assumed that the enemy was unsophisticated and that communications security did not warrant much concern (Myer, 1982: 64). Early policies were determined to be ineffective and time consuming to implement. Consequently, the ASA developed a new concept of "before the fact" assistance by having personnel serve as advisers rather than police officers. This new function emphasized the importance of planning operational communications procedures and the absolute necessity of communications security (Fennegan, 1998: 152). Basic techniques included changing call signs and frequencies and using codes for map coordinates. However, such techniques proved to be cumbersome and controversial due in part to the confusion of changes involving call signs and naming functions that were derogatory or degrading to U.S. Forces in the theater of operations (Myer, 1982: 65).

According to documentation compiled by Major General Joseph McChristian (1974) in his book, *Vietnam Studies: The role of Military Intelligence 1965-1967*:

> "The need for an accurate system to account for the large number of classified documents was a primary concern since the security of information was the focal point for the significant intelligence effort in the Republic of Vietnam."

Many initiatives and directives spawned from the security concerns during the Vietnam conflict. After the Counterintelligence division conducted command wide inventories of all classified material, it was determined there was a need to reduce the amount of classified material stored to decrease the likelihood of compromises.

The United States Military Assistance Command's (MAC) security policies and procedures provided key information on classified material that included the following:

- Number of classified documents
    - on hand at the beginning of the reporting period
    - on hand as the end of the reporting period
- Number of new documents generated
- Number destroyed
- Number dispatched
- Number downgraded.

Additionally, security control officers were trained to supervise overall security measures and practices and stress the importance of continuous security education (McChristian, 1974: 143). Even though the MAC established several policies and regulations governing COMSEC, many commanders disregarded the regulations and chose to sacrifice security considerations for speed and availability of communications. Such

decisions were much easier since satisfactory COMSEC often produced paralyzing confusion and an overall displeasure.

The establishment of Army Regulations 380-5, Safeguarding Defense Information, significantly improved the information security (INFOSEC) posture, *which* is the basis for the Command Information Security Program. In the early stages of this initiative, several instances revealed the lack of attention to detail, however, as the inspections became rapid, widespread improvements indicated that overall security training, education, and awareness increased command interest and helped to limit security violations and inconsistencies (McChristian, 1974: 145). This regulation and other initiatives provided an efficient security posture throughout the remainder of the conflict:

- Announced and unannounced inspections revealed inattention to basic security.
- Inspections and surveys improved the security posture of commands.
- Restrictive services served to remind all personnel of their security responsibility.
- Directives outlining the specific requirements for a security program.
- Full favorable personnel security investigations for Vietnamese applicants prior to employment in administrative, logistical, and custodial positions.
- Modified storage requirements to fit the capabilities of tactical units and advisory teams.
- Documents clearly marked with security classifications.
- The establishment of a “common need” for personnel access to sensitive data.

Other security devices enhanced the overall posture of the U.S. Military during the conflict. A key development was the implementation of the NESTOR family of narrowband secure voice equipment. Some devices included in the NESTOR family were, the KY-8 (Stationery Vehicle Use); KY-28 (Aircraft Use); and the KY-38 (Manpack or Mobile Use). Other devices, aimed at the mobility of military personnel, were the PRC-77 and VRC-12 used in combination with the KY-38 (Myer, 1982: 68-70).

In addition to the establishment of key INFOSEC regulations, the Vietnam Conflict brought major policy initiatives governing COMSEC. During the early stages of the war, COMSEC was a police-type function aimed at monitoring friendly communications and warning of possible compromises. This "after the fact" management of communication resources proved inefficient and at times, costly to military operations various activities. After such vulnerabilities were identified, the ASA progressed to a system that concentrated on "before the fact" assistance that led to the establishment of operational communications procedures and iterating the importance of COMSEC to military organizations (Finnegan, 1998; 152). During March 1970, the Military Assistance Command compiled a series of lessons learned outlining key issues effecting American Military units in Vietnam. According to *Vietnam Lessons Learned Number 79: Enemy exploitation of tactical communication* (USMAC, 1970), there were several problems with COMSEC:

> "The continuous employment of unauthorized codes, lack of proper communication discipline, and disregard of existing regulations, directives and specified procedures continue to provide the enemy with valuable and extremely timely intelligence information…..continued disregard for approved codes is constantly providing the enemy with timely intelligence which can be exploited for foil allied operations."

It is evident from the information provided from lessons learned documentation that more regulations with a greater emphasis was needed for "sound and secure communication techniques that strictly adhered to new and existing regulations" (USMAC, 1970).

The closing stages of Vietnam in 1973 occurred during the same time as the explosion of technologies related to the Internet, networking, and security become prevalent throughout the U.S. The significance of such events will continue to influence technological changes for the future and serve as a catalyst for military warfare. As the Internet became a catalyst for distributed systems, so did the need for greater security of information and information systems. The early history of the Internet highlights how increased use of Internet led to the identification of vulnerabilities discovered during events that could be considered unintentional acts that led to the identification of major concerns.

The History of the Internet

Although the U.S. Government was responsible for creating the predecessor to today's internet, it was not originally designed to transfer information critical to U.S. national security (Beauregard, 2001). However, today's internet is used for a seemingly infinite number of purposes, including key military communications and operations that enable the U.S. Military to maintain the highest level of combat readiness. Although internet related technology has changed how warfare is conducted, the use of information in war has been a basic warfighting requirement throughout history (Gumahad, 1997).

The history of the Internet provides an explanation of how IA programs evolved from necessary security measures taken by organizations. The Department of Defense

(DOD) is an organization that heavily relies on the Internet to conduct modern information operations. The protection and defense of information and information systems by ensuring their availability, integrity, identification, confidentiality, and non-repudiation was not a direct result of a single initiative but a continuous iteration of smaller -- individual efforts directed towards increased performance and efficiency systems we now know as the Internet. The Internet evolved over a very short period to become one of the most important systems available for military use. Even though modern IO is information and Internet intensive, early IO programs also focused on the protection of information from the enemy. This newer requirement will still focus on the core concept of protection.

The first signs of the need for increased protection and defense were not so obvious during the creation of the Internet in 1969. It began as the ARPANET, a major government and academic research institute in the United States funded by the Advanced Research Projects Agency (ARPA) of the U. S. Department of Defense (Hurd, 2001; Longstaff, 1997). The original goal was to create a network that would continue to function even if major sections of the network failed. Longstaff and others identified this concept as the rerouting of network traffic automatically around problems in connecting systems or in passing along necessary information. Such efforts were only seen as network openness and flexibility, which provided optimal services and performance to the small group of users.

As the affordable personal computer became available with the advent of smaller, more powerful computers, the 1980s saw an explosion in computer use by the average person (Hurd, 2001). In 1986, Cliff Stoll identified the first well-publicized international

security incident related to the Internet in his book, *The Cuckoo's Egg*. He identified an accounting error, which led him to uncover an international effort to exploit university and government computers by accessing and copying information from them (Stoll, 1989). According to Longstaff et al (1997), Stoll was the first to raise awareness to potential problems by identifying key ARPANET vulnerabilities that could be used for destructive purposes.

In 1988, Robert T. Morris, then a student at Cornell University, wrote a program that would connect to one computer another; find and use one of several vulnerabilities to copy itself to a second computer; and begin to run the copy of itself at the new location. A "worm" is the name of a computer program that automatically copies and replicates itself. Experts identified the Morris Worm was as the first automated network security incident against the ARPANET. The ARPANET extended to over 88,000 computers and was the primary means of communication among government network computer experts at the time of the incident. With the ARPANET effectively down, it was difficult to coordinate a response to the problem (Longstaff, 1997).

The network grew extensively over a short period and was vital to the daily operations of the ARPANET. It was important to find a way to prevent security disasters from occurring in the future. The solution was the creation of the Computer Emergency Response Team (CERT) coordination center to respond to network emergencies (Zakon, 2000). Today, CERT teams are widely known throughout the computer security world. Various teams from branches of the military coordinate responses to computer security incidents, assist sites in handling attacks, and educate network users about computer security threats and preventive practices.

The ARPANET officially became the Internet, the concept of a worldwide network of computers sharing information. It moved from a government research project to an operational network with over 100,000 computers in 1989 (Hurd, 2001; Zakon, 2000). Such rapid growth also led to more security incidents and new opportunities for additional network attacks. The growth of the internet prompted users to take a closer look at various security incidents and network attacks. Since the internet had become so valuable, it was necessary to take greater precautions to protect resources. The protection of resources was also a major problem since the many early network protocols that formed part of the internet infrastructure were designed without security in mind (Longstaff, 2000). This overall design made it difficult to manage various security aspects.

Security of the Internet and Information Systems

The exponential growth in internet security incidents from 1988 to 1995 demonstrates the importance of protecting the internet and information systems. According to experts, there are six reasons why the internet is vulnerable (Longstaff, 2000):

- Early network protocols designed without security in mind.
- Openness of the internet allows attacks to be quick, inexpensive and un-detectable.
- Sites have unwarranted trust and are unaware of the risks.
- Rapid development of internet related services and applications.
- Operating system security not considered at purchasing.

- Explosive growth has expanded the need for well-trained and experienced managers.

The six reasons identified above have caused organizations to take a closer look at the security of their systems. Figure 4 shows growth of the number of network security incidents from 1988 to 1995. The facts presented give justification for greater security measures of information and information systems.

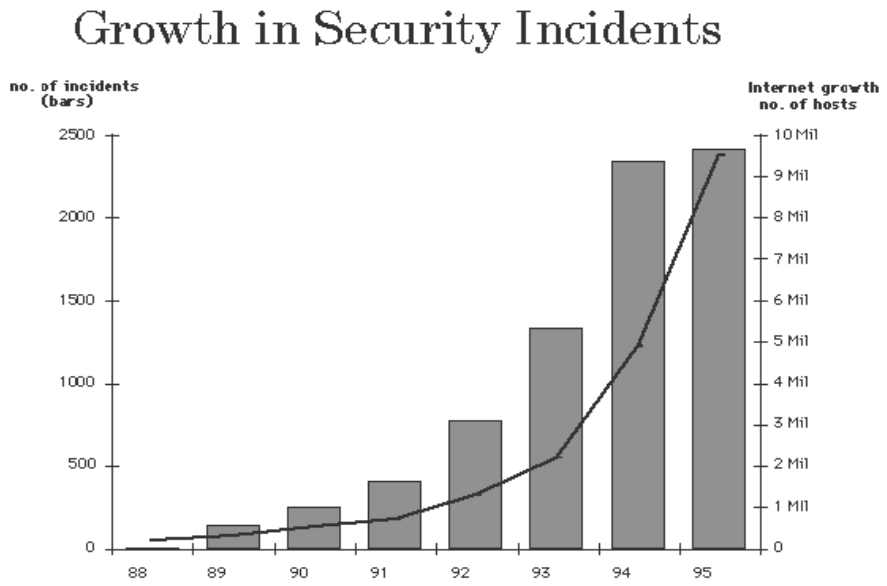

Figure 4: Security Incidents. 1988-1995 (CERT/CC, 2000)

This figure begins with the year 1988 and related data did not exist before this time. The protection of information in warfare has always been a key aspect of U.S. Military operations even though pertinent data related to the Internet is only available since 1988.

The military currently uses the internet for an infinite number of purposes. As Internet and Internet related technologies continue to revolutionize military operations, there are certain concepts developed over time that necessitate understanding of key warfare elements and the importance of protecting vital information and systems.

Because of this rapid growth, this necessity will further validate the importance of protecting pertinent information used for such purposes in the future.

Information Assurance Strategy

According to the *Air Force Doctrine Document* (AFDD) on *Information Operations,* IA is a subcategory of the Information Warfare (IW) under the Counter Information domain. The sub-domains of Offensive Counter Information (OCI) and Defensive Counter Information (DCI) form the nucleus of attack and defend operations performed during warfare. A recent research effort described this relationship:

> "Information Superiority gives the U.S. the ability to control information even on an insecure network such as the Internet. Since Information Superiority cannot be obtained and maintained without Information Assurance, to control the Information Operations spectrum the military must have the ability to protect its own information, detect any unauthorized intrusions, and react to those intrusions in a timely manner (Beauregard, 2001)."

OCI and DCI tactics, techniques, and procedures ensure significant advantage over adversaries and help to achieve military objectives aimed at IS (AFDD-1, 1998: 3). These two counter information categories, OCI and DCI, also exist simultaneously by protecting against potential vulnerabilities and exploiting the enemy's vulnerabilities.

IA focuses strictly on DCI tactics, techniques, and procedures that ensure protection, detection, and reaction to potential problems. The current IA structure makes the goal of information superiority easier to achieve. Although there are several other concepts represented under the DCI category, this research effort only focuses on the elements associated with IA since it is viewed as the

foundation of any defensive strategy for the protection of information and information systems (AFDD-1, 1998: 3).

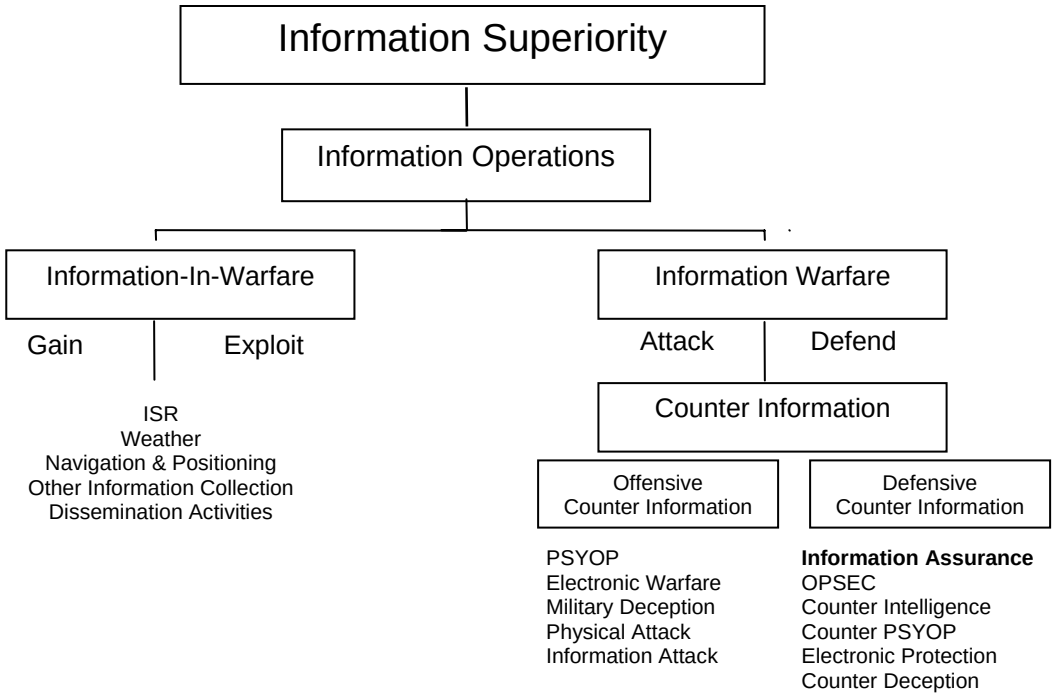

Figure 5: Air Force Information Superiority Construct (AFDD-1, 1998: 3)

The origins of the current IA structure and overall concept are embedded in earlier defensive strategies such as communications security (COMSEC) and information security (INFOSEC). According to the United States Marine Corps Institute's (USMCI) correspondence course on COMSEC (1998), it is a reversible weapon:

> "We will not win battles, unless our forces receive and preserve vital intelligence. We also cannot win battles, if the enemy receives this intelligence as readily as we do. Communications security, therefore, is an integral part of reliable communications which may prove to be the key to victory on the modern battlefield."

COMSEC is that protection resulting from all measures designed to deny unauthorized persons information of value from the study of communications. Essentially, the primary

purpose of COMSEC is to deny unauthorized persons or to protect valuable information obtained from studying communications. COMSEC is resultant of the need for military commanders to safeguard information during conflicts. Primarily, the U.S. Military has streamlined such concepts to achieve a certain level of reliable and secure communications. A balanced approach to the theory of COMSEC has four essential components of COMSEC: transmission security, physical security, cryptographic security, and emission security (USMCI, 1998).

- *Transmission security* is the protection of all transmissions and denial or reduction of the effectiveness of interception, traffic analysis, imitative deception, and radio direction finding.

- *Physical security* is the protection of classified communications equipment and material from unauthorized personnel.

- *Cryptographic security* is development and use of technically sound cryptosystems, and the application of proper crypto techniques.

- *Emission security* involves measures taken to deny unauthorized persons information of value that might be obtained from interception and analysis of compromising emanations from cryptographic and telecommunications systems.

The four components of COMSEC contribute to the protection of various systems, which is essential to IA concepts of confidentiality and integrity discussed in chapter one.

INFOSEC or information systems security is the protection of information systems against unauthorized access to or modification of information. This protection takes place against the denial of service to authorized users, whether in storage, processing or transit (Maconachy, Schou, and Welch, 2001). According to the approach taken by the authors, this historical definition of INFOSEC lacks stability as a stand alone concept under the current IA structure. Maconachy et al (2001) argued that INFOSEC

was an attempt to integrate separate disciplines like personal security, computer security and communications security into a coherent identifiable profession. Since INFOSEC primarily focuses on the protection of information and information systems from modification or disruptions in accessibility, it cannot support the larger spectrum of separate disciplines as originally intended. According to McCumber (1998), "even though COMSEC and INFOSEC provide system security support, merely combining these disciplines under an umbrella of common management will fail to capture an accurate view of this evolving technology." He advocated an approach that emphasizes the cornerstone of information systems security, information, and the technology that facilitates it.

Maconachy et al (2001), argued that the evolution of IA and the inception of the IA model began during the 1960's and progressed with the escalation of the information intensive environment of the late 1960's and beyond. There is clear evidence that demonstrates how many concepts of IA are present in the earliest military conflicts. Other examples demonstrate how information and information systems protection evolved during various military conflicts throughout American History. The information provided below will explore how IA approaches have origins in military conflicts from WWI through Vietnam.

Information Assurance Evolutionary Model Development

Applying the NSA IAM baseline categories to information presented earlier will assist in the development the overall plan to categorize concepts of the current evolutionary framework of IA. Additionally, the identification of key aspects of

Information States and Security Counter Measures previously explained by the McCumber IA model will influence the value obtained from the historical information. I will categorize previous technological mechanisms discovered from WWI through Vietnam to the present using the information states, security countermeasures, and the examples that correspond to each. According to Maconachy's theory and the NSA IAM baseline classification system, this categorization must also take place across the temporal domain. This explained by the forth dimension, as the forth dimension, time explains. Table 3, shows the temporal domain along with the IA model dimensions and the NSA IAM categories. This table will demonstrate early examples of information and information systems protection mechanisms during warfare.

Table 3: IA Evolution Model Core Elements

IA Model Dimensions	**WWI, WWII, Korea, Vietnam**	**NSA IAM Baseline Categories**
Information States	----------Time ----------	
Transmission		External Connectivity
Storage		Back-Ups Disposal
Processing		Auditing Session Controls
Security Counter Measures	Early Examples of Information and Information Systems Protection Mechanisms During Warfare	
Technology		Maintenance Telecommunications Virus Protection
Policies and Practices		Account Management Configuration Management Contingency Planning IA Documentation IA Roles & Responsibilities Media Sanitization
People	----------Time ----------	Awareness Personnel Security Physical Security Training

In addition to the three dimensions provided above, the representation of the security services dimension will address which of the five pillars; availability, authentication, confidentiality, integrity, and non-repudiation are more prevalent under each of the four wars. This dimension, along with indicators for IA in each war, is added after each category is presented across the temporal domain and during the final analysis of this research.

Justification

Temporal piece, developed from the Maconachy model and the NSA IAM, focuses on the period from WWI to Vietnam and those IA concepts common during military operations. Looking at the six stages of MIS historical research (McKenny, 1997) from chapter two, a crisis always ensued, which led to innovations and improvements in key areas. Wartime operations, or crisis and conflict, enhances the significance of overall war plans. This is the time when lessons learned and doctrinal changes are organized and the production working documents form key organizational changes. This notion is confirmed by the information contained in JP 3-13 (1998) on the IO function provided in chapter one. JP 3-13 demonstrated how IA was the only element of IO represented across the entire spectrum from peace, to crisis, to conflict, and to peace again with crisis and conflict being the critical timeframe.

Assumptions

The mapping of the baseline categories and the items listed under the Maconachy IA model under the proposed IA framework could fall into simultaneous areas or could

be defined differently in various literature depending on the specific criteria used. It is important to establish guidelines and focus on a common or major function and not by how each concept is implemented. The focus of this effort concentrated on the major functions of each concept to determine where each would fit in the development of the evolutionary model. The definitions of each dimension by Maconachy provided a general guideline for conducting a thorough categorization and will be used to formulate the various concepts of the evolutionary model explained below.

Approach to Model

Various lessons learned during warfare were attempts to outline actions taken to reduce the likelihood of security incidents linked to various leadership functions. The notion of speed or convenience versus security or inconvenience was a major issue. IA related concepts have been at the forefront of military operations during warfare. Operations are shaped by doctrinal changes that take place during and after a specific crises and outlined in lessons learned reports. Prior to additional classifications from the Maconachy model and the NSA IAM baseline, I will categorize previous technological mechanisms discovered from during the specific time frame covered using the information states and security counter measures dimensions.

The proposed model will provide discussion according to the sub-categories. Such a classification using the temporal domain will attempt to tie each of the wars with the four dimensions. Preceding each category discussion, I will provide a row vector of Maconachy IA model dimensions including the temporal addition and the segmentation of the pertinent details according to the NSA IAM - IA map.

Information States

The *transmission* state progressed steadily from a very basic function during WWI and WWII into a much more robust function during Korea and Vietnam. The primary theme was to provide accurate information to key entities in a timely and accurate manner. The radio was widely known as the sole source of electronic communications. The significance of the radio throughout the periods covered can be demonstrated by the wide use and the innovations to radio related technology over time. Table 4 demonstrates the transmission element across the temporal domain.

Table 4: Transmission Element

	World War I	World War II	Korea	Vietnam	Baseline
Transmission	Courier Dispatch Radio Tactical Telephone Telegraph	Couriers Radio Tactical Telephone Telegraph	Couriers Message Centers HF Radio Telephone	Message Centers VHF Radio (FM) Telephone	External Connectivity

The *storage* element continued to progress by gradually growing more streamlined with the introduction of new technologies to accommodate various changes over time. The storage dimension focuses on maintaining control and protecting an uninterrupted flow of information by keeping original copies in safe places (Maconachy, 2001). Early on, this process was manual and relied on the human element to provide system protection and availability. During Korea, a more progressive filing system and microfiche technology was developed and provided greater levels of security previously unavailable. Table 5 demonstrates the storage element across the temporal domain.

Table 5: Storage Element

	World War I	World War II	Korea	Vietnam	Baseline
Storage	Manual Archive - Locally	Manual Archive - File System Dev.	Microfiche - Systemized Archive - Formal Retrieval System Developed	Centralized Storage Fac. Magnetic Tape Paper Tape	Back-Ups Disposal

The *processing* element focuses on how information and information systems are protected during the preparation or interpretation stages (Maconachy, 2001). Coding and decoding expertise provided a primary means of processing various information. Even though coding and decoding provides either manual of automated functions, key elements focused on continuous improvement. The processing function has continued to be a key concern for military leadership, as demonstrated by examples taken from WWI and WWII. Later developments if this element focused on providing automated processes and centralized locations to conduct operations. Table 6 demonstrates the processing element across the temporal domain.

Table 6: Processing Element

	World War I	World War II	Korea	Vietnam	Baseline
Processing	Choctaw Talkers Manual-coding/decoding	Navajo Talkers Indian Talkers Manual - coding/decoding	Message Centers Semi-Automated - coding/decoding	Centralized - Message Processing Automated - coding/decoding	Auditing Session Controls

Security Counter Measures

The *technology* element includes many of the cryptographic systems of the past, which provided key advantages to both enemy and friendly combatants during warfare (Maconachy, 2001). During WWII, the U.S. military developed technologies and

improved on others developed elsewhere. Many of these technological advancements developed during WWII carried over to the Korean War. The Vietnam War also provided advancements in technology that led to internet related hardware and software developments. Table 7 demonstrates the technology element across the temporal domain.

Table 7: Technology Element

	World War I	World War II	Korea	Vietnam	Baseline
Technology	Scramblers - Shift Ciphers	Enigma Hagelin Ultra Bombes Purple SIGSALY M-209	SIGSALY M-209 SIAGBA	NESTOR (Secure Voice) - KY-8 - KY-28 - KY-38 - PRC-77 Transistors	Maintenance Telecommunications Virus Protection

The *policies and practices* element incorporates established procedures and concepts mandated by organizational leadership. This element continued to progress throughout American warfare and certain indicators demonstrate how prevalent certain concepts became as various wars progressed. Table 8 demonstrates the policies and practices element across the temporal domain.

Table 8: Policies and Practices Element

	World War I	World War II	Korea	Vietnam	Baseline
Policies and Practices	Encryption Code Books	Code Books COMINT Encryption SIGINT	Code Books COMINT Encryption INFO-OPS - Press Releases SIGINT	COMINT COMSEC Encryption INFOSEC Information Operations - Press Releases - Pol Pressure Press Releases OPSEC Security Policies - Encryption - Documents SIGINT TEMPEST	Account Management Configuration Management Contingency Planning IA Documentation IA Roles & Responsibilities Media Sanitization

The *people* element evolved from a decentralized structure to a more centralized one over time. The perception that people required awareness, literacy, training, and education led to a more centralized structure. As the need for greater role by communications leaders, so did the need for more structure governed by rules and regulations. Table 9 demonstrates the people element across the temporal domain.

Table 9: People Element

	World War I	World War II	Korea	Vietnam	Baseline
People	No Structure Decentralized	Decentralized Specialized Upper - Echelons	Centralized Training Programs Awareness Functions	Highly Centralized High Level Training Compliance - Enforcement	Awareness Personnel Security Physical Security Training

Security Services

The *security services* dimension focuses on the five key aspects of IA. Using the terms as defined earlier by this research effort, I categorized each by mapping the definition with the relevant examples provided throughout the information states and the security counter measures dimensions. An overall categorization that focuses on the key concepts identified throughout the proposed evolutionary framework. Indicators demonstrate that across the temporal domain, pertinent details of the current IA structure increased through time and led to the current structure of IA.

Table 10: Security Services Dimension

	World War I	World War II	Korea	Vietnam	Current
Security Services	Confidentiality Integrity	Availability Confidentiality Integrity	Availability Confidentiality Integrity	Authentication Availability Confidentiality Integrity	Authentication Availability Confidentiality Integrity Non-Repudiation

Chapter Overview

This chapter discussed current literature on the historical perspectives of warfare and the protection of information from World War I forward. This chapter also summarized background information pertinent to Information Operations (IO) strategies related to aspects of DCI and the IA domain as well as a brief history of the Internet and how advancements in networking technologies led to IA principles and practices. Finally, this chapter discussed the information assurance evolutionary process and its relationship to the warfare perspectives over time.

IV. Analysis

Introduction

The previous chapter explored current literature on the historical perspectives of warfare and the protection of information from World War I forward and summarized background information pertinent to Information Operations (IO) strategies related to aspects of Defensive Counter Information and the Information Assurance (IA) domain. This chapter will discuss the findings of this research effort by answering the research questions presented in chapter one.

Analysis of Historical Factors

Historical research takes into account past occurrences and their significant contribution to present and future events. Within the context of this research effort, past occurrences are examined to answer various questions proposed earlier. The following section will include information from previous chapters covering core elements of the evolutionary process.

Research Question One

The first research question asks, "What key programs were established to protect information and information systems in the U.S. Military from WWI through Vietnam to the present?" In order to answer this question, I analyzed pertinent documentation from each U.S. Military conflict since WWI. My research confirmed there were several programs established to protect information and information systems. Many served specific operational purposes. For example, several security devices of the Vietnam War

such as the Integrated Wideband Communications System addressed the need for high quality communications systems for high-speed data requirements. Other enhancements focused on the goal of increasing mobility of the war fighter while also increasing information security related functions (Rienzi, 1972).

The two main programs established to protect information and information systems were COMSEC and INFOSEC (McCumber, 2001). COMSEC is protection resulting from all measures designed to deny unauthorized persons information of value that is obtained from studying communications. Essentially, the primary purpose of COMSEC is to deny unauthorized persons or to protect valuable information obtained by using four essential security components; transmission security, physical security, cryptographic security, and emission security (USMCI, 1998). Even though the four essential components of COMSEC primarily deal with technical requirements, policies and practices established under this realm provide key functional areas by which detailed security plans were developed.

INFOSEC is the protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit and against the denial of service to authorized users. It also includes those measures necessary to detect, document, and counter threats. (Maconachy, 2001). INFOSEC focuses on the Information State dimensions discussed in the Maconachy IA model. This model provides justification that information resides in one or more of the three states at any given time. This is further validated by the evolutionary process examples identified during the military conflicts from WWI to Vietnam discussed in Chapter Three.

Research Question Two

The second research question asks, "What is an appropriate evolutionary model of IA given military operations from WWI through Vietnam to the present?" In order to answer this question, there must first be an overall outline of what information must be included. An appropriate IA evolutionary model should include the following:

- Incorporates historical perspectives with current criteria.
- Thoroughly defined approaches to historical data.
- Focuses on a specific period.
- Uses historical time and space.
- Incorporates the four dimensions discussed by McCumber and Maconachy.
- Focuses on the five pillars of current IA.
- Comprehensive approach to identifying key concepts.

I analyzed information presented from WWI to Vietnam in chapter three using the NSA IAM baseline categories as a foundation. This information covers the evolutionary processes related to IA that were prevalent in each military conflict. The model below demonstrates how the four dimensions; information states, security counter measures, and time were significant throughout American military warfare from WWI through Vietnam to the present. Additionally, the two dimensions show the significance of the baseline categories and the mapping to the Information States (transmission, storage, processing) and Security Counter Measures (technology, policies & practices, people). Since the mapping incorporates current concepts, the overall product should demonstrate the notion that older concept do relate to newer ones.

Table 11: IA Evolutionary Model (WWI to Vietnam)

	World War I	World War II	Korea	Vietnam	Baseline
Information States					
Transmission	Courier Dispatch Radio Tactical Telephone Telegraph	Couriers Radio Tactical Telephone Telegraph	Couriers Message Centers HF Radio Telephone	Message Centers VHF Radio (FM) Telephone	External Connectivity
Storage	Manual Archive - Locally	Manual Archive - File System Developed	Microfiche - Systemized Archive - Formal Retrieval Sys Developed	Centralized Storage Facilities Magnetic Tape Paper Tape	Back-Ups Disposal
Processing	Choctaw Talkers Manual- coding/decoding	Navajo Talkers Indian Talkers Manual - code/decode	Message Centers Semi-Automated - code/decode	Centralized - Message Processing Automated - code/decode	Auditing Session Controls
Counter Measures					
Technology	Scramblers - Shift Ciphers	Enigma, Hagelin Ultra Bombes, Purple SIGSALY M-209	SIGSALY M-209 SIAGBA	NESTOR (Secure Voice) - KY-8, - KY-28 - KY-38, - PRC-77 Transistors	Maintenance Telecommunications Virus Protection
Policies and Practices	Encryption Code Books	Code Books COMINT Encryption SIGINT	Code Books COMINT Encryption INFO-OPS - Press Releases SIGINT	COMINT, OMSEC Encryption, INFOSEC Information Operations - Press Releases - Pol Pressure Press Releases, OPSEC Security Policies - Encryption - Documents SIGINT, TEMPEST	Account Management Configuration Management Contingency Planning IA Documentation IA Roles & Responsibilities Media Sanitization
People	No Structure Decentralized	Decentralized Specialized Upper - Echelons	Centralized Training Programs Awareness Functions	Highly Centralized High Level Training Compliance -Enforcement	Awareness Personnel Security Physical Security Training
	World War I	**World War II**	**Korea**	**Vietnam**	**Baseline**
Security Services	Confidentiality Integrity	Availability Confidentiality Integrity	Availability Confidentiality Integrity	Authentication Availability Confidentiality Integrity	Authentication Availability Confidentiality Integrity Non-Repudiation

As discussed in the previous chapter, it is important to demonstrate what evolutionary processes are evident throughout the periods covered. This model shows pertinent details of each conflict, the corresponding information states and security counter measures, and the NSA IAM baseline categories. The model also demonstrates how current technologies form elements of the evolutionary time dimension, which coincide with each of the American wars. Finally, the model demonstrates the applicability of each of the four dimensions to the current framework structure.

V. Discussion, Limitations and Recommendations

Discussion

The goal of this research effort is to develop a historical account of events and concepts related to information and information systems protection during warfare. The previous chapter discussed the findings of this research effort by answering two of the three research questions presented in chapter one. This chapter will answer the final research question and discuss the conclusions, recommendations, and suggestions for future research.

Research Question Three

The third research question asks, "What lessons can we learn from the implementation of IA programs and the evolutionary model of IA? In order to answer this question, we have to focus on how the implementation of various IA programs over time affected overall outcomes. We can see from the historical cascade research approach that there are distinct events associated to this conceptual framework (McKenny, 1997).

1. Crisis
2. Search for a technical solution
3. Initial technical solution found
4. Adjustments throughout the organization
5. Assets formed, which resolves crisis
6. A dominant design

Every war started with a specific communication technology crisis. Such crisis stemmed from initial inadequacies identified during WWI. The ill-preparedness of the U.S. Military during WWII, Korea, and Vietnam stemmed form end of conflict cutbacks and the reallocation of funds to other more pertinent problems of the time.

Every crisis led to military leaders formulating ideals and innovations that developed into technical solutions. We can also see that policy drives the successful implementation of enhancements to security programs during warfare. Over the span of each specific conflict, adjustments were made to the initial technical solution to account for changes in plans and policies. A dominant design was produced once changes were incorporated and monies allocated for procurement of additional enhancements.

We can see from the evolutionary model presented earlier that advancements in technology have always driven the dominant design of any specific period. However, a specific dominant design may have been older technologies from previous conflicts utilized for the technical solution to newer crisis. For example, communications equipment used for the protection of information and information systems during WWII were also used during the early stages of the Korean War.

The exponential growth of security incidents fueled by technological changes will also demonstrate the future of IA related technologies, policies, and practices. Change in the future will happen much more quickly than in the past. The dominant design focus must shift from a reactive nature and focus on proactive leadership. Such leadership is beginning to take shape and several established programs demonstrate the emphasis on the future of the IA realm. Many programs center on training and certification, educations programs, and awareness functions. One example is the NSA's Information

Assurance Scholarship Program, which sponsors individuals to attend colleges and universities to study the full spectrum of IA. This program takes a proactive approach by training individuals in IA over the entire spectrum of their adult educational experience. This approach coupled with streamlined initiatives will dictate the overall effectiveness of future IA related issues.

Limitations

Since this research is concerned with a period spanning considerable frame of time, it is important to understand that the researcher was not present during the events presented. According to Bannister (2002), historical researchers do not have to be present when the events occurred, however, they must reconstruct and interpret events from a variety of sources and conceptualize the findings into a logical format for further interpretation.

This research also produces researcher bias. The information presented is the sole interpretation of the author who incorporated various historical methodologies, including inductive reasoning techniques, in order to produce snapshot of significant events of the past. Even though there is bias, the picture is complete as interpreted by the author. Thus, the final product provides a snapshot that deals primarily with the protection of information and systems during American warfare and how these concepts evolved into current IA structures.

Other examples of information and systems protection can be included as possible entities within the evolutionary model. However, due to time constraints of this thesis effort, the list provides a comprehensive view given the above control measures and a

focus on major concepts and practices aligned with the baseline categories and the IA model.

Suggestions for Future Research

This research effort focused on the warfare timeframe from WWI to Vietnam. Future research could expand the current information and focus on warfare after Vietnam through to the present Operation Enduring Freedom in Iraq. Although IA programs throughout the military have been steadily evolving since the adoption of various IA strategies, there are significant events and occurrences continue to shape IA as we know it. It would be beneficial to explore these later events to discover what specific changes have occurred. Additionally, such events will provide insight into what is in the future of IA programs across various strategic military spectrums.

Further research could also focus on a closer analysis of the various government policies implemented over the period covered by the evolutionary process. As these policies often involved technological advancements and practices, rapidly changing environments were seen as threats to smooth operational procedures and troop welfare. The implementation of various government policies also paved the way for the development of concepts and the overall applicability of the baseline categories and the Model dimensions. These policies stemmed from reactionary processes that favor an "after the fact" approach. It would be interesting to discover what pertinent details of policy creation will ensure that such occurrences and reactionary concepts do not occur in the future.

Conclusions

It is clear that significant events of past military warfare have shaped the current structure of military and civilian IA programs. Even though specific terms and views have changed or been re-designated, core concepts directly related to the NSA IAM baseline categories and the IA model were prevalent throughout the period covered. These concepts are still relevant and active in the current structure of IA. Additionally, these concepts and the entire evolutionary model demonstrate that the concept currently known as IA did in fact evolve from earlier forms of information and information systems security concepts during warfare. We can learn from these early examples and ultimately shape the future of IA by developing new concepts from those of the past.

Bibliography

Bannister, Frank. *"The Dimension of Time: Historigraphy in Information Systems Research."* Electronic Journal of Business Research Methods. Volume 1 Issue 1. 2002.

Barker, Wayne, G. The History of Codes and Ciphers in the United States During World War I. CA: Aegean Park Press, 1979.

Beauregard, Joseph, E., Modeling Information Assurance. MS thesis, AFIT/GOR/ENS. School of Engineering, Air Force Institute of Technology (AU), Wright Patterson AFB, OH, March 2001.

Boone, J.V. and R.R. Peterson. National Security Agency (NSA). *The Start of the Digital Revolution: SIGSALY Secure Digital Voice Communications in World War II.* Excerpt from published report. Fort Meade, MD: NSA, Oct. 13, 2000.

Borg, Walter, R., Gall, M., Gall, J. *Educational Research: An Introduction*. Pearson, Allyn & Bacon, 2002.

CERT/Coordination Center (CERT/CC). *Security of the Internet.* Pittsburgh: Carnegie Mellon Software Engineering Institute, 27 November 2000. n. pag. Excerpt from published report, http://www.cert.org/encyc_article/tocencyc.html.

Churchhouse, Robert. *Codes and Ciphers: Julius Caesar, the Egnima, and the Internet.* UK: Cambridge University Press, 2002.

DeGallaix, Henry M. *Destruction of the Brussels Radio Station*. Radio Amateur News, November 1919.

Denning, Dorothy, E., *Information Warfare and Security.* NY: ACM Press Books, 1999.

Department of Defense, Joint Chiefs of Staff. Joint Publication 3-13, *Joint Doctrine for Information Operations.* Washington: Pentagon, 9 October 1998.

Department of Defense. *Joint Vision 2020.* Washington DC: GPO, June 2000.

Diffie, Whitfield. Information Security: Where We Stand; Where We are Headed. Before the Subcommittee on Cybersecurity, Science, and Research and Development. Excerpt from unpublished report to the Select Committee on Homland Security, U.S. House of Representatives. July 15, 2003.

Finnegan, John, P. and Danysh, Romana. *Military Intelligence.* Washington DC: Center for Military History, U.S. Army. 1998.

Fishel, Edwin, C. *The Secret War for the Union.* NY: Houghton Mifflin, 1996.

Gumahad, A. T., II. "*The profession of arms in the Information Age*." Joint Force Quarterly: 14-20 (Spring 1997)

Hatch, David, A. and Benson, Robert, L. National Security Agency (NSA), *The Korean War: The SIGINT Background.* Excerpt from published report. Fort Meade, MD: NSA, June 28, 2000.

Hurd, Bryan, E. *"The Digital Economy and the Evolution of Information Assurance."* Proceedings of the IEEE: 252-257. June 2001.

Johnson, Thomas, R., National Security Agency (NSA), *Essay on the Korean War*. Excerpt from published report. Fort Meade, MD: NSA, September 28, 2000.

Kahn, David. *The Codebreakers: The Story of Secret Writing.* NY: Macmillan, 1967.

Kippenhahn, Rudolf. *Code Breaking, A History and Exploration*. NY: Overlook, 1999.

Knode, Monti, L. *Perceptions vs Reality: A Longitudinal Experiment in Influenced Judgment Performance.* MS Thesis, AFIT/GIR/ENV/03-09. School of Ingineering, Air Force Institute of Technology (AU), Wright Patterson AFB, OH, March 2003.

Kuhn, M.G. and Ross J. Anderson. "Soft Tempest: Hidden Data Transmissions Using Electromagnetic Emanations." Information Hiding: 1988.

Lee, J., Burke, C., and D. Anderson. *The US Bombes, NCR, Joseph Desch, and 600 Waves: The First Reunion of the US Naval Computing Machine Laboratory.* IEEE, Annals of the History of computing: July-September 2000.

Leedy, Paul, D. and Ormrod, Jeanne. *Research Planning and Design.* NY: Prentice Hall, 2000

Longstaff, T.A., Ellis, J.T., Herman, S. V., Lipson, H. F., McMillan, R. D., Pensante, L. H., and D. Simmel. *Security of the Internet*. Pittsburgh: Carnegie Mellon University, Software Engineering Institite, 1997. n. pag. Excerpt from published article, http://www.cert.org/encyc_article/tocencyc.html

Mason, R. O. and J.L. McKenney. "*Developing an Historical Tradition in MIS Research*." MIS Quarterly: Sept. 1997.

Mason, R. O., McKenney, J.L., and D.G. Copeland. *"An Historical Method for MIS Research: Steps and Assumptions."* MIS Quarterly: Sept. 1997.

McKnight, Walter, L. *"What is Information Assurance?"* CrossTalk: July 2002. http://www.stsc.hill.af.mil/crosstalk/2002/07/index.html.

Myer, Charles, R. LTGen, USA. *Vietnam Studies: Division Level Communications, 1962-1973.* Department of the Army. Washington, D.C.: 1982.

Montgomery, Bernard L. *History of Warfare.* Ohio: World Publishing, 1968.

Newton, David, E. *Encyclopedia of Cryptology.* California: ABC-CLIO, Inc., 1998.

Rienzi, T. M., LTGen, USA. *Vietnam Studies: Communications Electronics, 1962-1970.* Department of the Army, Washington, D.C.: 1972.

Smith, Michael. *The Emperor's Codes: The Breaking of Japan's Secret Ciphers*. NY: Arcade, 2000.

Stanford, M. *The Nature of Historical Knowledge.* Oxford: Blackwell, 1986.

Stoll, Clifford. *The Cuckoo's Egg.* NY: Doubleday, 1989.

Swanson, M. and B. Guttman. *Generally Accepted Principles and Practices for Securing Information Technology Systems.* National Institute of Standards and Technology (NIST), Technology Admin, U.S. Dept. of Commerce: September 1996.

United State Marine Corps Institute. *Communications Security.* Washington, DC: Marine Barracks, 26 Jan 1998.

Weadon, Patrick, D. National Security Agency (NSA), *The KoreanWar:* SIGINT and COMSEC Help Save the Day at Pusan. Excerpt from published report. Fort Meade, MD: NSA, September 18, 2000.

Weadon, Patrick, D. National Security Agency (NSA). *The SIGSALY Story*. Excerpt from published report. Fort Meade, MD: NSA, Oct. 13, 2000.

Westover, John, G. *Combat Support in Korea.* Washington, DC: U.S Army, 1987.

Wrixon, Fred, B. *Codes and Ciphers & Other Cryptic & Clandestine Communication.* NY: Black Dog & Leventhal, 1998.

Zakon, Robert H. "Hobbes' Internet Timeline v5.2." 19 November 2000. Excerpt from published article, http//info.isoc.org/guest/zakon/internet/History/Hit.html.

Vita

Gunnery Sergeant Kelvin Bernard Scott enlisted in the Marine Corps and attended Recruit Training at Parris Island, South Carolina in June 1988. He holds a BS from the University of Maryland and a MS from Troy State University.

He attended the Basic Supply Course at Marine Corps Logistics Base, Albany Georgia. In December 1988, he transferred to MCAS Kaneohe Bay, Hawaii. In support of Operation Desert Shield and Desert Storm during the Persian Gulf War, Corporal Scott embarked aboard the USS Tripoli and the USS Tarawa for duty. In February 1992, he reported to Marine Corps Security Force (MCSF) Training Battalion in Chesapeake, Virginia and was later assigned to MCSF Company, London, England. During his tour in London, he served as Sergeant of the Guard, and Color Sergeant. Additionally, he was voted as Marine of the Year and Meritoriously Promoted to Sergeant. In July 1995, he was assigned to the Third Force Service Support Group, Okinawa, Japan. During hs tour on Okinawa, he served a variety of positions within supply and management field. In September 1999, Staff Sergeant Scott reported to the Marine Security Guard School at Quantico, Virginia and was later assigned as the Detachment Commander of Marine Security Guard Detachments, Dakar, Senegal and Bangkok, Thailand.

In August 2002, Gunnery Sergeant Scott entered the Graduate School of Engineering and Management at the Air Force Institute of Technology. Upon graduation, he will be assigned as the Information Assurance Manager, Headquarters III Marine Expeditionary Force, Okinawa, Japan. He is married and they have two children.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From – To)*
03-12-2004	Master's Thesis	Jun 2003 – Mar 2004

4. TITLE AND SUBTITLE

AN ANALYSIS OF FACTORS THAT HAVE INFLUENCED THE EVOLUTION OF

INFORMATION ASSURANCE FROM WORLD WAR I THROUGH VIETNAM TO THE PRESENT

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Scott, Kelvin, B., Gunnery Sergeant, USMC

5d. PROJECT NUMBER
If funded, enter ENR #

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)
Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 P Street, Building 640
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT/GIR/ENV/04M-22

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
HQMC, C4
Attn: Master Sergeant Dulany
2 Navy Annex
Washington, DC 20380-1775 Phone: 703-693-3490 Email: dulanykm@hqmc.usmc.mil

10. SPONSOR/MONITOR'S ACRONYM(S)
HQMC C4

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES

14. ABSTRACT
This study is an exploratory historical analysis of the factors that have influenced the evolution of military Information Assurance (IA) programs from World War I to the present. Although the term IA has recently been widely used throughout the Information Resource Management field (IRM), evidence indicates that information and information systems protection mechanisms were used during every U.S. Military conflict. This research proposes to increase the body of knowledge within the information systems management field by exploring the areas related to Information Assurance (IA) and the ultimate goal of U. S. Defensive Information Warfare.

I found that significant events related to the protection of information and information systems security throughout each U.S. Military conflict led to the implementation of IA concepts. The evaluation of these events provides key information that reveals a common approach to IA throughout history and supports the identification of key concepts that have influenced this evolutionary process and shaped the role of IA in current military operations, with indicators of how it may be used in the future.

15. SUBJECT TERMS
Information Assurance, History, Evolution, INFOSEC, COMSEC, Communications, WWI, WWII, Korea, Vietnam and Internet History

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
REPORT	**ABSTRACT**	**c. THIS PAGE**			Alan R. Heminger, PhD, AFIT/ENV
U	**U**	**U**	**UU**	85	**19b. TELEPHONE NUMBER** *(Include area code)* (937) 785-3636 Ext. 4797 alan.heminger@afit.edu